1. What is aws?

AWS stands for Amazon Web Service; it is a collection of remote computing services also known as cloud computing platform. This new realm of cloud computing is also known as IaaS or Infrastructure as a Service.

1. Layers of cloud computing

IaaS, PaaS, SaaS and Business Process Outsourcing(BPO)

1. Difference between scalability and flexibility

Scalability is the ability to increase or decrease IT resources as needed to meet changing demand.

Flexibility is the ability to access systems and data quickly and easily.

1. Difference between Amazon MarketPlace AMIs and AWS QuickStarts?

AWS Marketplace AMIs provide single-vendor solutions that run on EC2 instances. In contrast, AWS Quick Starts are modular and more customizable solutions that might (or might not) use Amazon EC2.

1. Events triggered by Amazon CloudFront.

Viewer Request, Viewer Response, Origin Request, and Origin Response.

1. What are the features of EC2?

Bare metal instances

Pause & resume facility

High IO

Flexible storage option

Elastic IP address

Enhanced networking

1. Difference between elastic and public IP

Elastic IP address is a reserved public IP address that you can assign to any EC2 instance in a particular region, until you choose to release it

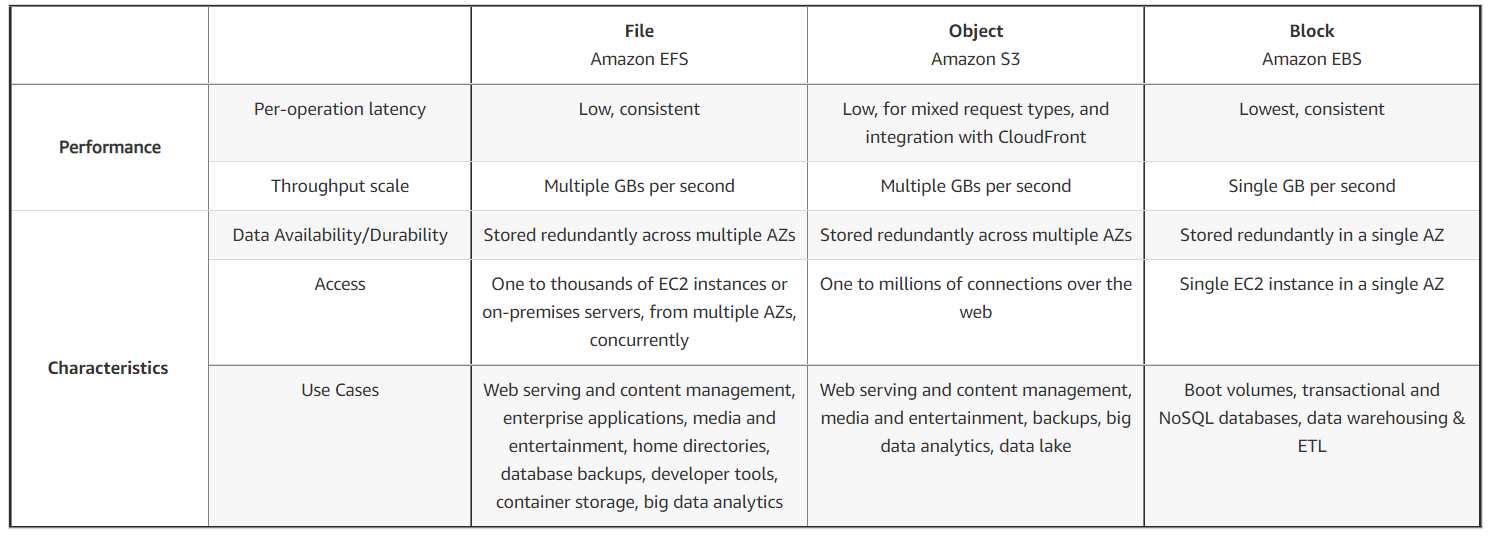
It is unique for the account not just the instance, so if instance is terminated and restarted, elastic IP does not change.

1. Comparison between EBS, EFS and S3.

Amazon EFS is a file storage service for use with Amazon compute (EC2, containers, serverless) and on-premises servers. Amazon EFS provides a file system interface, file system access semantics (such as strong consistency and file locking), and concurrently-accessible storage for up to thousands of Amazon EC2 instances.

Amazon EBS is a block level storage service for use with Amazon EC2. Amazon EBS can deliver performance for workloads that require the lowest-latency access to data from a single EC2 instance.

Amazon S3 is an object storage service. Amazon S3 makes data available through an Internet API that can be accessed anywhere.



1. What happens when you launch instances in Amazon VPC ?

When you launch an EC2 instance into a VPC, the subnet has to be specified in which to launch the instance. The Amazon EC2 launch wizard in the Amazon EC2 console can be used to launch your instance.

1. Can I vertically scale Amazon EC2 instance?

Yes, but for that the instance needs to be restarted or replaced with a new instance, which will require a downtime. We can use AWS Ops Automator to automatically scale EC2 instance .

1. Differentiate between vertical and horizontal scaling in AWS.

Horizontal Scaling involves in changing the number of nodes in a computing system whereas Vertical Scaling helps in increasing the size and computing power of a single instance or node without affecting others.

1. What is the total number of buckets that can be created in AWS by default ?

By default, can be created 100 buckets in each AWS accounts and can be increased up to 1000 by submitting a service limit increase.

1. Difference between RDS, Redshift and DynamoDB

Both Amazon Redshift and Amazon RDS enable you to run traditional relational databases in the cloud while offloading database administration. Customers use Amazon RDS databases primarily for online-transaction processing (OLTP) workload while Redshift is used primarily for reporting and analytics.

1. How can you send request to Amazon S3 ?

Request sending can be done using the REST API or the AWS SDK wrapper libraries that wrap the Amazon S3 REST API by simplifying the programming tasks in Amazon s3.

1. What Is Lambda@edge In Aws?

Lambda@Edge is a feature of Amazon CloudFront which allows running code that improves performance and reduces latency by making them globally distributed all with zero server

administration.

1. What are the steps followed in AWS EC2 creation?

* Creating Key Pair
* Creating Security Groups
* Choose Launch Instance
* Choose instance type
* Configure instance details
  + Number of instances
  + Purchasing option
  + Network – choose VPC used in SG
  + Choose default subnet in any availability zone
  + Choose File system
  + Check user data, it should have commands for mounting the file system
* Add Storage
* Add Tags
* Add the above created security group in Configure Security Group by selecting existing security group option
* Choose launch

1. What is an AMI?

AMI is a template that contains a software configuration (for example, an operating system, an application server and applications). From an AMI, an EC2 instance can be launched, which is a copy of the AMI running as a virtual server in the cloud.

You can launch multiple instances of an AMI.

You can create an AMI from an existing EC2 instance.

1. What are different types of instances?

Compute, Storage, memory optimized and accelerated computing

1. What is DDoS attack and how can it be prevented in AWS?

DDoS means distributed denial of service, it attacks network, transport, presentation and application layer and makes services unavailable for the intended end users.

We can prevent this using following services in AWS.

* Limiting access points by using load balancers and CDNs(Content Distribution Network)
* Adding firewalls or using Access Control Lists(ACLs) to limit what traffic reaches to application
* Using AWS WAF against attacks like SQL injection or cross-site request forgery.

AWS services that we can use are:

* Shield
* WAF
* ELB
* Route53
* Cloudfront
* VPC – Using Security group at different level.
  + The SSH bastion is a single Amazon EC2 instance used to provide secure administrator access and hosting only a Secure Shell (SSH) service
  + Elastic Load Balancing (ELB) allows you to achieve greater fault tolerance by automatically routing inbound traffic across multiple Amazon EC2 instances.
  + With a NAT instance, you can securely route traffic from private subnets out to the Internet, while denying any inbound connectivity from the Internet.
  + Network ACLs provide an additional layer of defense for your VPC by allowing you to create stateless allow and deny rules that are processed in numeric order, much like a traditional firewall. This is useful for allowing or denying traffic at a subnet level, as opposed to security groups that allow traffic at an EC2 instance level.

1. What rule is needed for you to be able to connect to EC2 via putty shell?

In SG, inbound rules, we need SSH Type, and My IP as Source.

1. What is the purpose of using security groups?

SGs act as firewall for associated instances, controlling both inbound and outbound traffic at the instance level.

You must add rules to a SG that enable you to connect to your instance from your IP address using SSH.

You can also add rules that allow inbound and outbound HTTP and HTTPS access from anywhere.

If you plan to launch instances in multiple regions, you will need to create a SG in each region.

1. Difference between terminating and stopping an EC2 instance

Terminating an EC2 instance will remove any attached EBS volumes and delete them.

1. Difference between dynamic and auto scaling

Dynamic scaling responds to changing demand and predictive scaling automatically schedules the right number of EC2 instances based on predicted demand.

1. Difference between on demand and spot instances.

A spot instance is an instance that uses spare EC2 capacity that is available for less than the On Demand price.

Spot instances are very well suited for data analysis, batch jobs, and optional tasks.

If timeout is not specified, the spot instance request continues to automatically make the launch request until the capacity becomes available.

The hourly price of spot instances varies based on demand, for on-demand instances it is fixed.

1. Why choose Glacier/Deep Archive over standard storage class?

Glacier costs 0.004 cent per GB and Deep Archive costs 0.0009 cents per GB. Which makes both options cheaper as compared to any other storage class.

These are used to store objects that do not require frequent access and can be archived.

1. How can you control the access to S3 data?

Block Public Access, IAM policies, Bucket Policies, Access Control Lists, S3 Access Points, Presigned URLs, AWS Trusted Advisor.

1. How can you enforce object deletion security measures?

You can enable versioning and multi factor authentication on bucket.

1. How can you automate the process of S3 bucket creation?

Using yaml scripts as templated in cloud formation or using boto3 in python.

1. How can you move the versioned objects from one storage class to another?

In python code, you can use the property NoncurrentVersionTransition to move to another class and NoncurrentVersionExpiration to delete the older version.

1. How does aws determine the noncurrent version of an object in S3?

AWS determines the duration of noncurrent version by checking the date of creation of its successor.

1. How can you define an object transition to another class and expiration after the movement?

Using Transition property and Expiration property respectively

1. How can you apply rules to specific folders in a bucket?

You can use Filter tags to apply filters, within which you can use tags like prefix to filter of folders starting with a string value.

This can be used to define different rules for different keys.

1. Write an xml code to move current object to Standard-IA in 90 days, versioned (old copies) to S3 Glacier in 30 days and delete old copies in 365 days

<LifecycleConfiguration>

<Rule>

<ID>Sample\_Rule</ID>

<Status>Enabled</Status>

<Transition>

<Days>90</Days>

<StorageClass>Standard\_IA</StorageClass>

</Transition>

<NoncurrentVersionTransition>

<Days>30</Days>

<StorageClass>S3 Glacier</StorageClass>

</NoncurrentVersionTransition>

<NoncurrentVersionTermination>

<Days>365</Days>

</NoncurrentVersionTermination>

</Rule>

</LifecycleConfiguration>

Yaml Code:

LifecycleConfiguration:

Rules:

- Id: Sample\_Rule

Status: Enabled

Transitions:

- TransitionInDays: 90

StorageClass: STANDARD\_IA

NoncurrentVersionTransitions:

- TransitionInDays: 90

StorageClass: GLACIER

NoncurrentVersionExpirationInDays: 365

1. What permissions can be given to S3 bucket in management console for AWS?

LifeCycleConfiguration, ReplicationConfiguration and InventoryConfiguration.

1. What are the different types of server side encryptions available in S3?

SSE-S3 : Requires that amazon S3 manage the data and encryption keys

SSE-C : Requires that you manage the data and encryption keys and Amazon S3 manages the encryption and decryption alone, not the keys

SSE-KMS : Requires that you manage the customer master key(if not provided, S3 creates an AWS managed CMK) and S3 manages the data encryption keys

1. When to use SSE-S3 vs SSE-KMS?

SSE KMS is preferred when you need more control over the encryption keys.

Amazon S3 provides strongest cipher(256-bit advanced encryption standard AES-256) and rotates the master key regularly that it uses to encrypt the key used for encrypting all objects.

SSE KMS provides additional features like audit trail on who used CMK and when and separate permissions for the use of a CMK.

S3 only accepts symmetric keys.

1. When would you prefer an asymmetric CMK?

Only in the cases when you don’t need automatic key rotation and don’t need to integrate with AWS services and your use case requires encryption outside of AWS by users who cannot call AWS KMS.

1. Difference between symmetric and asymmetric CMK.

Symmetric CMK represents a 256-bit encryption key that never leaves AWS KMS unencrypted.

Asymmetric CMK is a mathematically related public and private key pair where you can give the public key to anyone but private key remains a secret and never leaves AWS KMS unencrypted.

1. How can you get the ARN of an already created aws kms CMK?

In the kms console -> Choose Customer Managed Keys or AWS managed keys - > Select the alias/Key ID -> In general configuration you can see the ARN for this key.

1. What do you understand by KMS option in Key material origin for a key?

It is a property of CMK that identified the source of the key material in the CMK. If it is KMS, automatic rotation of key is possible. Possible values are : KMS, External and CloudHSM

1. What do you mean by multi region key?

When you create a key, you can select if you want it to be a multi region key, it essentially means that there will be a primary private key and it will be replicated across multiple regions and it will ideally be the same with just a small difference in the arn, it will have the arn of the region in which it is replicated.

These are useful when you have data spanning across multiple regions and you have cross replication enabled. Or when there is an AWS region outage, multi region keys let you process encrypted data without interruption.

1. What is IAM?

AWS Identity and Access Management (IAM) is a web service that helps you securely control access to AWS resources for your users. You use IAM to control who can use your AWS resources (authentication) and what resources they can use and in what ways (authorization).